Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 32 (2014) 571 – 578

Procedia Computer Science

5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)

Implementation of A3ACKs intrusion detection system under various mobility speeds

Abdulsalam Basabaa[a], Tarek Sheltami[a] and Elhadi Shakshuki[b]

[a] *King Fahd University of Petroleum & Minerals, Dhahran, 31261, Saudi Arabia*
[b] *Jodrey School of Computer Science, Acadia University, Nova Scotia, B4P 2R6, Canada*

Abstract

Wireless networking is an emerging technology that allows users to access information and services anywhere regardless of their geographic location. Mobile Ad hoc Network (MANETs) is one of the most significant technologies among various wireless communication technologies. In MANETs, all nodes are mobile and can be connected dynamically using wireless link in a random manner. All nodes work as routers and take part in discovery and maintenance of routes to other nodes in the network. MANETs are unique infrastructure less network and have self-configuring features make them suitable for many critical applications, such as military and emergency applications. However, these features make them also vulnerable for all types of passive and active attacks because of open environment, the rapidly changing topology and the decentralization of nodes. In addition, most of the proposed protocols assume that all nodes in the network are cooperative, and do not address security issues. Moreover, most of the proposed existing intrusion detection systems (IDSs) of are based on Watchdog technique. In this paper, we propose and implement a new intrusion detection system named Adaptive three ACKnowledgments (A3ACKs) that solves three significant problems of Watchdog technique, mainly: receiver collision, limited transmission power and collaborative attacks. We use Network Simulator 2 (NS2) to implement and test our proposed system under different networks with various mobility speeds as well as compare our results with the results of some closely existing IDSs mechanism.

Keywords: Mobile Ad hoc NETwork (MANETs); Intrusion Detetion System(IDS); Adaptive Acknowledgement (AACK);Adaptive Three Acknowledement Intrusion Detetion System (A3ACKs).

1. Introduction

Wireless networks have much growth comparing with traditional wired network due to their unique architecture and features. As a result, wireless networks are replacing traditional wired networks everywhere and in different

Corresponding Author. Tel.:+966554840169; E-mail address: g201002320@kfupm.edu.sa

doi:10.1016/j.procs.2014.05.462

applications. One of the most important applications of wireless networks is Mobile Ad-hoc NETwork (MANET). MANET is defined as an infrastructure-less network that is self-configuring mobile nodes connected by wireless links either directly or indirectly. In MANETs, each node has wireless transmitter and receiver. Thus, each node in MANETs can communicate directly with other nodes if they are within the communication range (called single-hop MANET). Otherwise, they are relay on each other to forward packets to their final destination when they are out of communication range (called multi-hop MANET). In addition, mobile nodes inside MANETs are free to move randomly [1]. More details about MANETs can be found in [2-5]. Unlike traditional wireless network or wired network, MANET is infrastructure-less and non-centralized network. These features make MANETs suitable for many applications that need quick deployment and minimal configuration, such as military or disaster recovery [6] [7]. On the other hand, MANETs are vulnerable to all types of passive and active attacks due to the open environment, the rapidly changing topology and distribution of nodes in MANETs. Furthermore, most of the proposed MANET protocols assume that all nodes in the network are cooperative, and do not address security issues in MANETs. Furthermore, most of the existing IDSs that are designed especially for MANETs are based on Watchdog mechanism and they have several weaknesses.

In our previous work, we developed an intrusion detection system that is able to detect misbehaving nodes in MANETs without presence of collaborative misbehaving nodes in a route path [8]. In this paper, we extend our work by proposing and implementing a novel IDS named Adaptive three ACKnowledgments (A3ACKs) that solves three significant problems of Watchdog technique, which are receiver collision, limited transmission power and collaborative attacks especially within presence of two consecutive collaborative attacks in a route path in MANETs. We implement and test our proposed system under different networks with various mobility speeds as well as compare our results with AACK [16] [17].

The remainder of this paper is organized as follows; in section 2 we present related work with their pros and cons. In section 3, we describe the proposed scheme (A3ACKs) in details. The performance evaluations and results of A3ACKs IDS are presented in section 4. Finally, the conclusions in Section 5.

2. Related work

Traditional centralized monitoring techniques are not appropriate for MANETs due to their different architecture and changing topology [9]. As a result, it is essential to design and develop intrusion detection systems (IDSs) mainly for MANETs. May research have been done related to this topic [10] [11] [12]. More details about intrusion detection systems in MANETs can be found in our previous work [13]. In this section, we concentrate on Watchdog and Pathrater techniques and their drawbacks as our research targets to solve their disadvantages. Lastly, we describe TWOACK and AACK technique as they are more closely to our research in this paper.

2.1. Watchdog and Pathrater

Marti et al. [14] proposed Watchdog technique as well as Pathrater techniques in 2000 that improve network performance within presence of misbehaving nodes. Watchdog uses to detect misbehaving nodes in a network that agree to forward packets but fail to do so, while Pathrater technique uses to avoid these misbehaving nodes in a route path in the future transmission. The integrating of Watchdog and Pathrater techniques improve network performance significantly [14] in MANETs. Watchdog technique detects the misbehaving nodes by applying promiscuous mode, where each node listens to its neighbor transmissions. If the next node in a route path fails to forward the sent packet, it increases its failure counter. Then it determines the node as misbehaving if the failure counter exceeds a certain predefine threshold. As a result, the Pathrater technique avoids this node in the future transmission by cooperating with routing protocol to choose different path from source to destination depending on the used algorithm. Even though Watchdog and Pathrater techniques are able to detect misbehaving nodes at forward level instead of the link level, it may fail to detect misbehaving nodes within the presence of: 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior report, 5) collusion (collaborative) of malicious nodes, and 6) partial dropping. In this paper, our goal is to solve three of these six weaknesses, named, receiver collisions, limited transmission power and collaborative misbehaving nodes in a route path. Details about these weaknesses as follow:

- **Receiver collisions**: Node A assure that node B has forwarded packet 1 to node C by overhearing, but fails to detect that node C didn't receive packet 1 due to a collision of packet 1 with packet 2 forwarded by node X. That means, both nodes B and X are trying to send packet 1 and packet 2, respectively, to node C at the same time as shown in Figure 1.

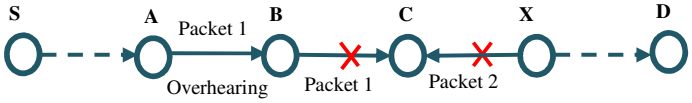

Figure 1: Receiver Collisions

- **Limited transmission power**: In order to save energy, a misbehaving node could limit its transmission power such that the signal is strong enough to be overheard by the previous node, but too weak to be received by the true recipient. For example, node B could limit its transmission power so it is strong enough to be overheard by node A but too weak to be received by node C, as shown in Figure 2.

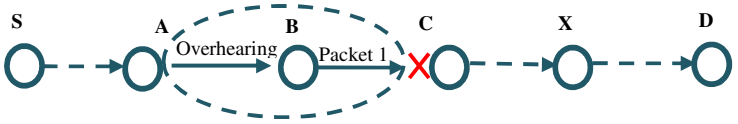

Figure 2: Limited Transmission Power

- **Collaborative attacks (collusion attacks)**: Multiple misbehaving nodes in MANETs could cooperate to drop packets instead of forwarding them. For example, nodes B and C in Figure 3 could cooperative to drop packet 1, where node B forwards packet 1 to node C but does not report to node A when node C drops packet 1.

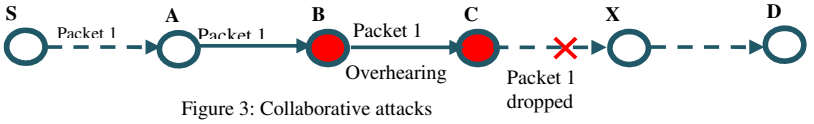

Figure 3: Collaborative attacks

2.2. TWOACK

The TWOACK technique is a network layer acknowledgment scheme proposed by Balakrishnan et al. [15]. TWACK replace Watchdog scheme by solving two of its weaknesses, named, receiver collision and limited transmission power. In TWOACK, when node forward a packet to its neighbor in a route path, it has to validate whether the packet successfully received by the node that is two hops from it. This achieved by acknowledging every data packet transmitted from source to destination over every three consecutive nodes along the path. As shown in figure 4, node B receives packet 1 from A and forwards it to C, node C (two hops away from A down the route) is required to generate acknowledgement packet (TWOACK). When node C sends the TWOACK packet back to A indicates that B has forwarded packet 1 to C successfully. If A didn't receive TWOACK packet from C within a predefined timeout, then node A marks nodes B and C as misbehaving nodes. This process carries out for every three consecutive nodes along the rest of route path.

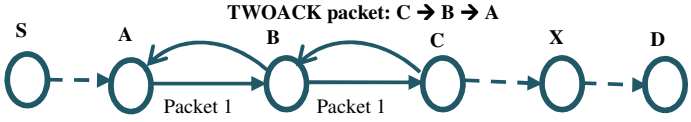

Figure 4: TWOACK scheme

The advantage and disadvantage of TWACK scheme were discussed in [15]. The advantage of TWOACK scheme is that it is able to detect misbehaving nodes with the presence of receiver collision and limited transmission power. However, the disadvantage of TWOACK technique is that it generates more overhead and reduces network performance due to acknowledgment every data packet on the route path. Moreover, it detects misbehaving links

instead of misbehaving nodes. This enable misbehaving nodes continue defect network performance as they have more time before detecting them.

2.3. AACK

AACK technique is an enhancement scheme to TWOACK technique proposed by Sheltami et al. [16] and Al-Roubaie et al. [17]. It is network layer acknowledgment based scheme consists of two models: TWOACK model and End-to End acknowledgment model (AACK). It is designed especially for MANETs and it aims to solve two problems of Watchdog technique, named, receiver collision and limited transmission power with less overhead comparing with TWOACK technique. The AACK scheme is stand for Adaptive Acknowledgment scheme since it has two parts (TWOACK and End-to-End) controlled by switching system. In AACK scheme, the default model of switching system is End-to-End acknowledgment (AACK) model where source node S sends data packet to destination node D on an active path without any overhead except one bit indicates packet type i.e. AACK or TACK as shown in figure 5. After destination node receives the sent data packet (packet 1), it must generate an AACK packet (acknowledgment packet) and sends it back to the source node in opposite direction of active route path. If the source node S didn't receive the AACK packet within predefined timeout from destination node D, the source node S has to switch to TACK model to detect if there is misbehaving nodes in route path.

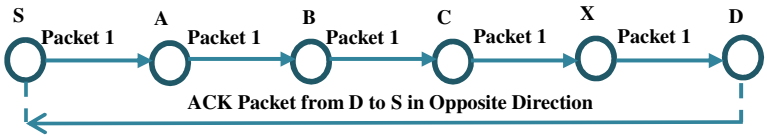

Figure 5: AACK model of AACK scheme

The TACK model, in AACK scheme, works similar to TWOACK scheme [15] except that it detects misbehaving nodes in a route path instead of links. Even though AACK techniques uses hybrid models (AACK and TACK) to detect misbehaving nodes in a route path with less overhead unlike TWOACK technique, AACK still suffers from detect malicious nodes within the presence of collaborative attacks in a route path.

3. Scheme description

Our proposed Adaptive Three ACKnowledgements (A3ACKs) scheme is an extension of the AACK scheme. It aims to solves three weaknesses of the Watchdog scheme, which are limited transmission power, receiver collision and collaborative attacks (collusion attack) especially if there are two consecutive collaborative misbehaving nodes in a route path. In this scheme we assume that the misbehaving nodes cooperative to forward routing packet but they drop data packets. The A3ACKs technique is an acknowledgement-based scheme based on Dynamic Source Routing Protocol (DSR) [18]. It consists of three main models, named, End-To-End Acknowledgement (Aack) model, Two Acknowledgement (Tack) model and Three Acknowledgment (Thack) model. The data packet in each model is different according to flag indicator as shown in Table 1, where we use only 2 bit of DSR reserved header in order to classify packet types for each model.

Table 1: Packet Type Indicator for A3ACK Scheme.

Packet Type	Aack	Tack	Thack
Packet Flag	01	10	11

In the A3ACK, the default model is Aack model which is similar to AACK mode in AACK scheme [16][17] as shown in figure 5, where the source node S first sends data packet to destination node D along the active route that is gets from DSR routing protocol. Also, the source node S has to register the sending packet ID and sending time. When destination D receives the sending data packet, it has to generate an Aack packet and sends it back to the source node on the same route path but in opposite direction. If the source node S didn't receive the Aack packet with predefined timeout, it has to switch to Tack model to detect if there is any misbehaving nodes in active route path. The Tack model works similar to TWOACK scheme, as discussed in section 2 (related work), except that it

detects misbehaving nodes instead of links. In Tack model, the third node for every three consecutive nodes in route path has to send back a Tack packet to first node. This process carries out by every three consecutive nodes in a route path as shown in figure 4. If the source node S fails to receive acknowledgement packet (Tack) within a predefined timeout, it has to switch to Thack model to detect if there are any collaborative misbehaving nodes in the route path. The Thack model aims to solve the problems of receiver collision and limited transmission power and collaborative attacks as well within presence of two consecutive misbehaving nodes in a route path. In the Thack model, every four consecutive nodes in path work together where the fourth node (three hops away from the first one) has to send back an Thack packet to the first node in that group within a predefined time out, as in shown in Figure 6.

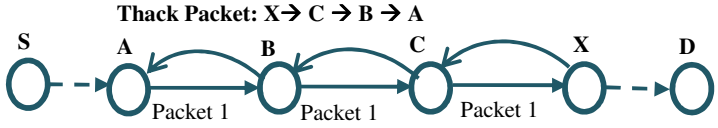

Figure 6: Thack mode: Each node is required to send back an acknowl- edgement packet to the node that is three hops away from it.

For example, if node C receives packet 1 from node B and forwards it to node X, node X (three hops away form A) has to generate a Thack packet with a reverse route path from A to X, and sends it back to node A indicating both nodes B and C have forwarded packet 1 to X successfully. If node A didn't receive the Thack packet from X within predefined timeout, node A reports that nodes B and C as misbehaving nodes. This process repeated for every four consecutive nodes along the route path. By adaption these three models, our proposed A3ACKs technique ables to solve all of receiver collision, limited transmission power and the collaborative attacks problems especially if there are two consecutive misbehaving nodes in a route path.

4. Performance evaluations

4.1. Simulation methodology

Our simulation environment created using Network Simulator (NS2), version 2.34 on Ubuntu 10.10 run on laptop with Core 2Duo CPU and 4GB RAM. We adapted NS 2.34 default scenario to contain 50 nodes scattered on 670 x 670 m flat area. The Random Waypoint mobility used with pause time zero and nodes moving speeds are 1 m/s for low speed network, and 20m/s for high speed network. Physical layer and 802.11 MAC layer are used in wireless extension of NS2. We used User Datagram Protocol (UDP) traffic with Constant Data Rate (CBR) 4 packets/second and packet size 512 B. In each network (low speed or high speed) and for each scenario, the simulation runs 10 times with various seed number from 1 to 10 and fixed run time 900 seconds. After that, the average value was calculated. Finally, misbehaving nodes were generated and scattered randomly from 0% to 40% with a scale increment equal to 10%.

In order to evaluate our A3ACKs technique, we tested it under two types of networks: *low speed network* and *high speed network*. In addition, we implemented two different types of scenarios for misbehaving nodes (MN) in each network. *Scenario 1*: we configured network simulator to let certain nodes work as misbehaving nodes that drop all data packets they receive. The objective of this scenario is to tests the performance of A3ACKs scheme against two drawbacks of Watchdog, which are receiver collision and limited transmission power, without the presence of collaborative attacks. Scenario 2: we configured network simulator to let certain nodes work as smart collaborative packet dropping misbehaving nodes, where these nodes cooperate together for dropping data packets and forward the routing packets. Moreover, when misbehaving nodes drop packets they send back acknowledgement (Tack) packets in opposite direction to the sender that is two hops away from them. The goal from this scenario is to test the performance of the A3ACKs scheme against receiver collision, limited transmission power and collaborative attacks weaknesses of Watchdog IDS especially within presence of two consecutive misbehaving nodes in a path. To measure A3ACKs performance, we use the same metrics [17] [19]:

- *Packet Delivery Ratio* (*PDR*): It defines the ratio of number of received packets at destination node to number of sent packets by the source node.

- *Routing Overhead* (*RO*): It defines ratio of routing related packets [Route Request (RREQ), Route Reply (RREP), Route Error (RERR), Aack, Tack, and Thack] in bytes to total routing and data transmissions in bytes in whole network.

4.2. Simulation results and discussions

In this section, we make a comparison between the results of the new A3ACKs scheme and the existing AACK scheme in low speed network and high speed network for scenario 1 and 2. Figure 7 compares the results of packets delivery ratio (PDR) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes for scenario 1. It is clear that the PDR of AACK and A3ACKs schemes almost the same in scenario 1 for low speed network and as well as for high speed network. However, PDR for both A3ACKs and AACK schemes in low speed network is higher than that in high speed network due to the stability in low speed network. As a result, more packets are delivered to destination nodes. But in general, PDR for A3ACKs and AACK schemes increase if misbehaving node ratio decrease.

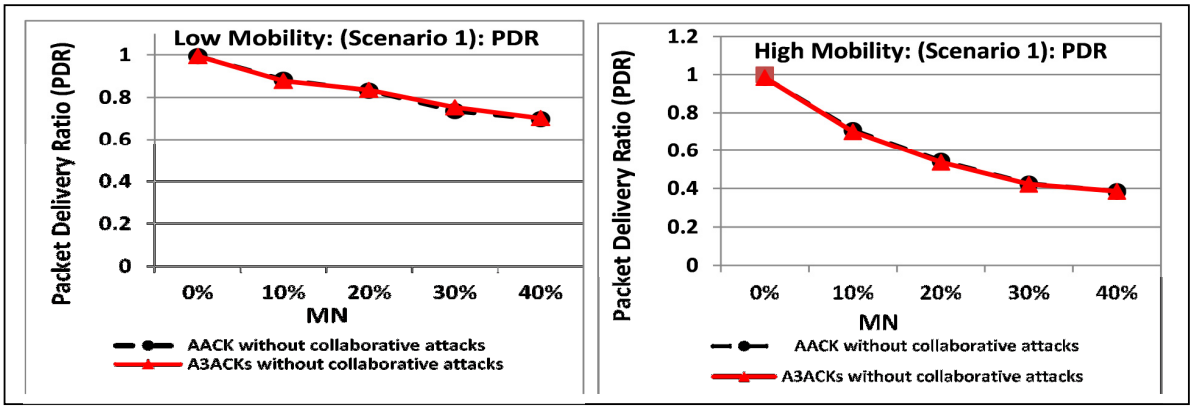

Figure 7: Comparison the results of PDR vs. MN ratio for A3ACKs and AACK scheme in low and high speed networks for scenario 1

Figure 8 compares the results of Routing Overhead (RO) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes also for scenario 1. Again it is clear that the RO of AACK and A3ACKs schemes almost the same in scenario 1 for low speed network and for high speed network as well. On the other hand, RO for both A3ACKs and AACK schemes in low speed network is lower than that in high speed network due to the stability in low speed network, so less packets are dropped and low overhead. PDR is inversely proportional to RO for both A3ACKs and AACK schemes.

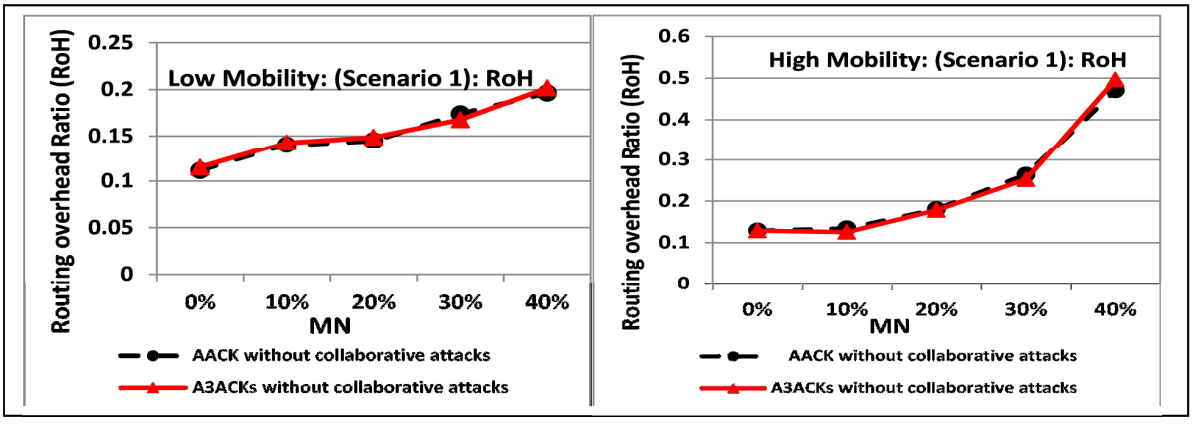

Figure 8: Comparison the results of RO ratio vs. MN ratio for A3ACKs and AACK scheme in low and high speed networks for scenario 1

Figure 9 compares the results of packets delivery ratio (PDR) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes for scenario 2. For high speed network, A3ACKs slightly tops AACK scheme when MN ratio is between 10% and 20%. Whereas, the PDR of A3ACKs scheme outperforms AACK scheme by approximately 11% to 16% when MN between 30% and 40% respectively. Also, for low speed network, A3ACKs is slightly better AACK scheme slightly when MN ratio is between 10% and 20%. However, A3ACKs surpasses AACK by about 10% and 13% when MN ratio is between 30% and 40% respectively. PDR for both A3ACKs and AACK scheme in low speed network is higher than that in high speed network due to the stability in low speed network.

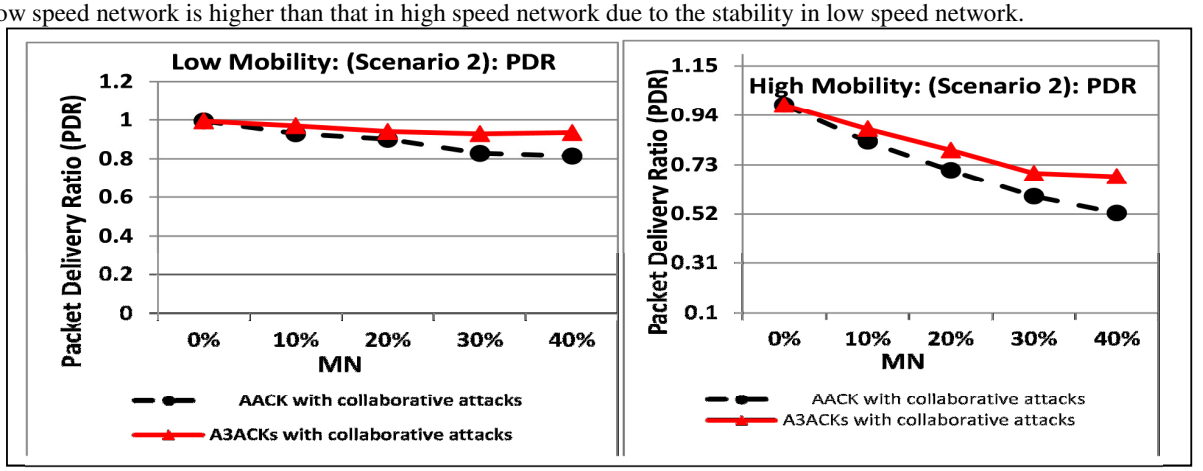

Figure 9: Comparison the results of PDR vs. MN ratio for A3ACKs and AACK scheme in low and high speed networks for scenario 2

Figure 10 compares the results of Routing Overhead (RO) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes for scenario 2. In general, RO for both AACK and A3ACKs schemes are increased if the MN ratio increases in both high speed network and low speed network. In case of high speed network, it is clear that the RO of A3ACKs scheme is higher than AACK scheme especially at 40% MN. This could be as a result of using the Thack model, as previously discussed, in A3ACKs technique to detect collaborative MN in a path when Tack model fails to detect them. As a result, this leads to increase RO of A3ACKs scheme compared with AACK scheme. In case of both low and high speed networks, AACK scheme is slightly better than A3ACKs scheme at 40%. However, RO for both A3ACKs and AACK scheme in low speed network is lower than that in high speed network due to stability in low speed network.

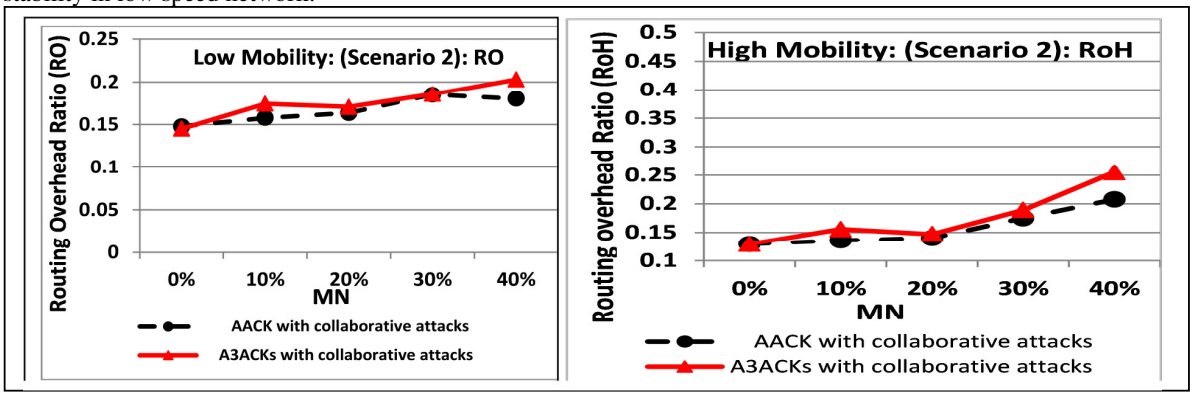

Figure 10: Comparison the results of RO ratio vs. MN ratio for A3ACKs and AACK scheme in low and high speed networks for scenario 2

5. Conclusion

In this research paper, we proposed enhanced IDS scheme for MANETs mainly: A3ACKs. We tested it under low speed and high speed networks using DSR protocol and we compared the results against our previous work. The results show that the A3ACKs improved network performance with or without the presence of consecutive collaborative misbehaving nodes in a route path for both low speed and high speed networks. Even though the network routing overhead has slightly increased the network security is more robust, and we think this trade-off is justified.

Acknowledgement

This research supports by King Fahd University of Petroleum and Minerals (KFUPM) and Acadia University.

References

[1] Jayakumar, G and Gopinath, G. 2007. Ad Hoc Mobile Wireless Networks Routing Protocol – A Review. In Journal of Computer Science 3(8): 574-582.

[2] C. E. Perkins, Ad-hoc Networking. Addison Wesley Professional, December 2000.

[3] M. Ilyas, ed., The Handbook of Ad-hoc Wireless Networks. CRC Press, December 2002.

[4] Hekmat, Ramin . Ad-hoc Networks: Fundamental Properties and Network Topologies. Netherlands: Springer , 2006. pp.154. eBook.

[5] M. Barbeau, E. Kranakis, Principles of Ad-hoc Networking. Wiley, 2007.

[6] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[7] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24-28, 2007, pp. 1154-1159.

[8] Shakshuki, E., Kang, N., Sheltami, T., "EAACK – A Secure Intrusion Detection System for MANETs", IEEE Transactions on Industrial Electronics, vol. 60, no., pp. 1089-1098, 2013.

[9] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[10] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf. Pervasive Comput. Commun., 2005, pp. 191–199.

[11] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[12] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[13] N. Kang, E. M. Shakshuki and T. R. Sheltami. Detecting Misbehaving Nodes in MANETs, the 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), November, Paris, France.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[15] Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137-2142 Vol. 4, 13-17 March 2005.

[16] T. Sheltami, A. Al-Roubaiey, E. Shakshuki and A. Mohmoud. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, 273-282. 2009.

[17] Al-Roubaiey, A.; Sheltami, T.; Mahmoud, A.; Shakshuki, E.; Mouftah, H., "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.634-640, 20-23April2010.

[18] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[19] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.